# Explicit Criteria for Quintic Residuacity 

By Kenneth S. Williams*


#### Abstract

Let $p$ be a prime $\equiv 1(\bmod 5)$. Necessary and sufficient conditions are determined for the prime $q(q \leqslant 19)$ to be a quintic residue of $p$. The results for $q \leqslant 7$ are known, the rest are new.


Throughout this paper $k$ is an odd prime and $p$ is a prime $\equiv 1(\bmod k)$ say, $p=$ $k f+1$. The $f$-nomial periods are defined by

$$
\begin{equation*}
\eta_{s}=\sum_{r=0}^{f-1} \exp \left(2 \pi i g^{k r+s} / p\right) \quad(s=0,1, \ldots, k-1) \tag{1}
\end{equation*}
$$

where $g$ is a primitive root $(\bmod p)$. The period equation $P_{k}(t)$ of degree $k$ is defined by

$$
\begin{equation*}
P_{k}(t)=\prod_{s=0}^{k-1}\left(t-\eta_{s}\right) . \tag{2}
\end{equation*}
$$

It is well known that $P_{\boldsymbol{k}}(t)$ has integral coefficients (see for example [12, p. 194]).
Since replacing the primitive root $g$ in (1) by another primitive root merely permutes the $\eta_{i}$, the coefficients of $P_{k}(t)$ are independent of the choice of $g$. The discriminant $D_{k}$ of $P_{k}(t)$ is also an integer independent of $g$ given by

$$
\begin{equation*}
D_{k}=\prod_{0 \leqslant r<s \leqslant k-1}\left(\eta_{r}-\eta_{s}\right)^{2} . \tag{3}
\end{equation*}
$$

The following is essentially a theorem of Kummer [6] (see also Lehmer [8], [10]).
Theorem 1. (i) A prime $q(\neq p)$ not dividing $D_{k}$ is a kth power residue of $p$ if and only if the congruence $P_{k}(t) \equiv 0(\bmod q)$ is solvable.
(ii) Every prime $q(\neq p)$ dividing $D_{k}$ is a kth power residue of $p$.

When $k=3$ it is well known (see for example [12, p. 223]) that

$$
\begin{equation*}
P_{3}(t)=t^{3}+t^{2}-\frac{1}{3}(p-1) t-\frac{1}{27}(p L+3 p-1), \quad D_{3}=p^{2} M^{2} \tag{4}
\end{equation*}
$$

where the integers $L, M$ satisfy

$$
\begin{equation*}
4 p=L^{2}+27 M^{2}, \quad L \equiv 1 \quad(\bmod 3) \tag{5}
\end{equation*}
$$

Theorem 1 can be used in conjunction with (4) and (5) to give explicit necessary and sufficient conditions for a prime $q$ to be a cubic residue of $p$ in terms of congruences

[^0]$(\bmod q)$ involving $L$ and $M$. For example, we find that 2 is a cubic residue of $p$ if and only if $M \equiv 0(\bmod 2)$, that 3 is a cubic residue of $p$ if and only if $M \equiv 0(\bmod 3)$, that 5 is a cubic residue of $p$ if and only if $L$ or $M \equiv 0(\bmod 5)$, etc. Such conditions have been given by Jacobi [5] for $q \leqslant 37$ and for $q \leqslant 47$ by Cunningham and Gosset [2].

In this note we consider the case $k=5$. Lehmer [7] has shown that

$$
\begin{equation*}
P_{5}(t)=t^{5}+t^{4}+c_{3} t^{3}+c_{2} t^{2}+c_{1} t+c_{0} \tag{6}
\end{equation*}
$$

where the integers $c_{0}, c_{1}, c_{2}, c_{3}$ are given by

$$
\left\{\begin{align*}
5 c_{3}= & -2(p-1)  \tag{7}\\
25 c_{2}= & -(6 p+p x-2) \\
500 c_{1}= & -\left[p\left(x^{2}-125 w^{2}+8 x-4 p+24\right)-4\right] \\
25000 c_{0}= & -p\left[x^{3}+10 x^{2}-1250 w^{2}+625 w\left(u^{2}-v^{2}\right)+40 x+80\right] \\
& +8 p^{2}(x+5)+8
\end{align*}\right.
$$

where $(x, u, v, w)$ is a solution of

$$
\left\{\begin{array}{l}
16 p=x^{2}+50 u^{2}+50 v^{2}+125 w^{2}, \quad x \equiv 1 \quad(\bmod 5)  \tag{8}\\
x w=v^{2}-4 u v-u^{2}
\end{array}\right.
$$

Dickson [3] has shown that (8) is always solvable; and that if $(x, u, v, w)$ is a solution, all the solutions are $(x, u, v, w),(x,-u,-v, w),(x, v,-u,-w)$ and $(x,-v, u,-w)$. If the condition $x \equiv 1(\bmod 5)$ is dropped, the only other solutions of $(8)$ are the negatives of those given above. In [10] Lehmer gives

$$
\begin{equation*}
256 D_{5}=p^{4}\left[w^{2}(4 v-3 u)-u(u-v)^{2}\right]^{2}\left[w^{2}(3 v+4 u)+v(u+v)^{2}\right]^{2} \tag{9}
\end{equation*}
$$

Theorem 1 can be used in conjunction with (6), (7), (8), (9) to give explicit necessary and sufficient conditions for a prime $q$ to be a quintic residue of $p$ in terms of congruences $(\bmod q)$ involving $x, u, v, w$. As there are a great many cases involved (depending on the residue classes $(\bmod q)$ of $p, x, u, v, w)$ in doing this even for small primes $q$, Carleton University's Xerox Data Systems Sigma- 9 computer was programmed to carry out the details for $q=2,3,5,7,11,13,17,19$. As the results are known for $q=2,3,5,7$ (by different methods), we illustrate the ideas involved by just giving some of the details in the case $q=11$. In order to do this we introduce the following notation. If $a, b, c, d$ are any integers, we let

$$
\begin{align*}
{[a, b, c, d]=} & \{(a, b, c, d),(a,-b,-c, d),(a, c,-b,-d),(a,-c, b,-d)  \tag{10}\\
& (-a,-b,-c,-d),(-a, b, c,-d),(-a,-c, b, d),(-a, c,-b, d)\}
\end{align*}
$$

and write $(x, u, v, w) \in[a, b, c, d](\bmod q)$ to mean $(x, u, v, w) \equiv(f, g, h, i)(\bmod q)$ for some $(f, g, h, i) \in[a, b, c, d]$. The computer showed in the case $q=11, p \equiv 1$ $(\bmod 11)$, that $D_{5} \equiv 0(\bmod 11)$ if and only if

$$
(x, u, v, w) \in[0,0,0,2],[4,0,0,0] \quad \text { or } \quad[4,2,4,6](\bmod 11)
$$

| q | $\left(\frac{p}{q}\right)$ | w $\equiv 0$ ( mod q) | $\begin{gathered} w \neq 0 \quad(\bmod q) \\ (u / w, v / w) \quad(\bmod q) \end{gathered}$ |
| :---: | :---: | :---: | :---: |
| 2 |  | $\mathrm{x} \equiv \mathrm{u} \equiv \mathrm{v} \equiv 0$ |  |
| 3 | +1 | $\mathrm{x} \neq 0, \mathrm{u} \equiv \mathrm{v} \equiv 0$ |  |
|  | -1 |  | $(0,0)$ |
| 5 | +1 | $\mathrm{x} \neq 0, \mathrm{u} \equiv \mathrm{v} \equiv 0$ | $(1,3)$ |
| 7 | +1 | $\mathrm{x} \neq 0, \mathrm{u} \equiv \mathrm{v} \equiv 0$ | $(1,2)$ |
|  | -1 |  | $(0,0),(0,2)$ |
| 11 | +1 | $\mathrm{x} \neq 0, \mathrm{u} \equiv \mathrm{v} \equiv 0$ | $(0,0),(0,4),(3,4)$ |
|  | -1 | $\mathrm{x} \equiv 0, \mathrm{u} \equiv 2 \mathrm{v}$ | $(1,1),(1,4)$ |
| 13 | +1 | $\mathrm{x} \neq 0, \mathrm{u} \equiv \mathrm{v} \equiv 0$ | $(0,6),(1,4),(3,8),(4,7)$ |
|  | -1 |  | $(0,0),(1,8),(2,8),(3,6),(3,7)$ |
| 17 | +1 | $x \neq 0, u \equiv v \equiv 0$ | $\begin{aligned} & (1,11),(2,2),(2,6),(2,14),(3,3) \\ & (3,12),(4,9) \end{aligned}$ |
|  | -1 |  | $\begin{aligned} & (0,0),(1,14),(2,7),(2,9),(2,10) \\ & (4,7),(4,10),(5,9) \end{aligned}$ |
| 19 | +1 | $\begin{array}{ll} x \neq 0, & u \equiv v \equiv 0 \\ x \equiv 0, & u \equiv 7 v \end{array}$ | $\begin{aligned} & (0,0),(0,9),(1,6),(1,7),(1,9) \\ & (4,9),(5,11),(6,8),(7,7),(8,9) \end{aligned}$ |
|  | -1 | $\mathrm{x} \neq 0, \mathrm{u} \equiv 7 \mathrm{v}$ | $\begin{aligned} & (0,4),(1,1),(1,12) *,(1,13),(2,7) \\ & (2,11),(6,7),(6,12),(9,9) \end{aligned}$ |

${ }^{*}$ In this case $x \equiv 0(\bmod 19)$.
All congruences are taken modulo $q$. We note that when $q$ is odd and $u \equiv v \equiv 0, w \neq 0$ $(\bmod q)$ then $x \equiv 0(\bmod q)$.
and that $D_{5} \not \equiv 0(\bmod 11)$ with $P_{5}(t) \equiv 0(\bmod 11)$ solvable, if and only if

$$
(x, u, v, w) \in[1,0,3,9] \quad(\bmod 11)
$$

where $(x, u, v, w)$ is any solution of (8). Thus, in this case, by Theorem 1,11 is a quintic residue of $p$ if and only if

$$
(x, u, v, w) \in[0,0,0,2],[4,0,0,0],[1,0,3,9] \quad \text { or } \quad[4,2,4,6](\bmod 11)
$$

that is, if and only if some solution $(x, u, v, w)$ of (8) satisfies

$$
u \equiv v \equiv 0 \quad(\bmod 11)
$$

$$
u \equiv 0, \quad v \equiv 4 w, \quad w \not \equiv 0 \quad(\bmod 11)
$$

or

$$
u \equiv 3 w, \quad v \equiv 4 w, \quad w \not \equiv 0 \quad(\bmod 11) .
$$

In this manner the following theorem was obtained.
Theorem 2. Let $p$ be a prime $\equiv 1(\bmod 5)$, and let $q$ be one of $2,3,5,7,11$, $13,17,19$. Then $q$ is a quintic residue of $p$ if and only if some solution $(x, u, v, w)$ of (8) satisfies the conditions given in the preceding table.

Table of primes $\equiv 1(\bmod 5)$ and $<10,000$
having $2,3,5,7,11,13,17,19$ as quintic residues

| 2 |  |  | 3 |  |  | 5 |  |  |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| 151 | 3881 | 8831 | 41 | 3881 | 9011 | 31 | 4861 | 9311 |
| 241 | 4211 | 9041 | 431 | 4051 | 9221 | 191 | 5051 | 9341 |
| 251 | 4751 | 9091 | 491 | 4111 | 9341 | 251 | 5281 | 9491 |
| 431 | 4861 | 9431 | 661 | 4201 | 9421 | 271 | 5471 | 9531 |
| 571 | 4871 | 9461 | 761 | 4721 | 9851 | 601 | 5591 | 9561 |
| 641 | 4931 | 9511 | 1021 | 4801 |  | 641 | 5711 | 9851 |
| 911 | 5021 | 9521 | 1051 | 4951 |  | 761 | 6211 |  |
| 971 | 5381 | 9781 | 1091 | 5351 |  | 1091 | 6271 |  |
| 1181 | 5441 |  | 1171 | 5501 |  | 1861 | 6421 |  |
| 1811 | 5471 |  | 1471 | 5591 |  | 2381 | 6581 |  |
| 2011 | 5581 |  | 1511 | 6011 |  | 2521 | 6701 |  |
| 2351 | 5641 |  | 1871 | 6091 |  | 2621 | 6791 |  |
| 2381 | 5711 |  | 2111 | 6101 |  | 2741 | 6951 |  |
| 2411 | 5821 |  | 2131 | 6301 |  | 2851 | 6971 |  |
| 2731 | 5861 |  | 2161 | 6311 |  | 3061 | 6991 |  |
| 3051 | 6221 |  | 2281 | 6421 |  | 3121 | 7151 |  |
| 3121 | 6361 | , | 2441 | 6481 |  | 3461 | 7691 |  |
| 3221 | 6571 |  | 2521 | 6521 |  | 3581 | 7901 |  |
| 3251 | 6581 |  | 2591 | 6581 |  | 3631 | 8581 |  |
| 3301 | 6791 |  | 2621 | 6701 |  | 3701 | 8681 |  |
| 3331 | 6871 |  | 2791 | 6991 |  | 4001 | 8731 |  |
| 3361 | 8161 |  | 2851 | 7331 |  | 4201 | 8861 |  |
| 3391 | 8191 |  | 3191 | 7451 |  | 4261 | 8951 |  |
| 3541 | 8461 |  | 3221 | 7591 |  | 4271 | 8971 |  |
| 3761 | 8501 |  | 3691 | 8101 |  | 4421 | 9011 |  |
| 3821 | 8681 |  | 3851 | 8831 |  | 4591 | 9221 |  |


| 7 |  |  | 11 |  |  | 13 |  |  |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| 181 | 3881 | 9781 | 61 | 3881 | 9341 | 61 | 3361 | 8191 |
| 311 | 4091 | 9851 | 191 | 3931 | 9391 | 271 | 3491 | 8221 |
| 661 | 4111 | 9901 | 241 | 4001 | 9661 | 311 | 3541 | 8311 |
| 811 | 4241 |  | 311 | 4111 | 9811 | 331 | 4021 | 8461 |
| 911 | 4391 |  | 541 | 4211 |  | 461 | 4391 | 8641 |
| 971 | 4441 |  | 66.1 | 4241 |  | 601 | 4591 | 8761 |
| 1031 | 4591 |  | 691 | 4261 |  | 761 | 4621 | 9091 |
| 1151 | 4861 |  | 751 | 4621 |  | 971 | 4651 | 9281 |
| 1171 | 5011 |  | 911 | 4951 |  | 1021 | 4751 | 9421 |
| 1201 | 5051 |  | 1181 | 5381 |  | 1061 | 4831 | 9491 |
| 1321 | 5261 |  | 1231 | 5431 |  | 1091 | 5011 | 9511 |
| 1621 | 5441 |  | 1291 | 5441 |  | 1151 | 5231 | 9521 |
| 1811 | 5591 |  | 1301 | 5471 |  | 1381 | 5281 | 9781 |
| 1861 | 6,451 |  | 1481 | 5531 |  | 1481 | 5431 |  |
| 1871 | 6761 |  | 1531 | 5741 |  | 1571 | 5651 |  |
| 2161 | 6841 |  | 1871 | 6151 |  | 1601 | 572.7. |  |
| 2371 | 6871 |  | 1931 | 6311 |  | 174.1 | 6301 |  |
| 2381 | 7411 |  | 2351 | 6421 |  | 1861 | 6451 |  |
| 2441 | 7451 |  | 2521 | 6481 |  | 2142 | 6551 |  |
| 2741 | 7561 |  | 2591 | 7211 |  | 2251 | 6581 |  |
| 2801 | 8191 |  | 2741 | 7321 |  | 2281 | 6691 |  |
| 3011 | 8431 |  | 2791 | 7351 |  | 2714 | 7001 |  |
| 3361 | 8861 |  | 3001 | 7541 |  | 3001 | 7321 |  |
| 346, | 9281 |  | 3301 | 7901 |  | 3012 | 7351 |  |
| 36,31 | 9491 |  | 3461 | 8221 |  | 3191 | 7681 |  |
| 3691 | 9511 |  | 3701 | 9001 |  | 3221 | 8171 |  |

The results for $k=2,3,5$ are due to Lehmer [10] (see also [7], [9] , [14]). The result for $k=7$ is a simpler restatement of a restatement due to Lehmer [10] of a theorem of Muskat [13]. The rest are new.

A table giving the values of $(x, u, v, w)$ corresponding to primes $p \leqslant 10,000$, $p \equiv 1(\bmod 5)$ has been deposited by the author in the UMT file of the American Mathematical Society. Using this table and Theorem 2, it was found that out of the 306 primes $p \leqslant 10,000$ with $p \equiv 1(\bmod 5) ; 60($ resp. $57,58,55,56,65,67,77)$ of them have 2 (resp. $3,5,7,11,13,17,19$ ) as a quintic residue of $p$. The actual

| 17 |  |  | 19 |  |  |
| ---: | :---: | :---: | :---: | :---: | :---: |
| 101 | 2791 | 8461 | 131 | 3331 | 7331 |
| 181 | 2801 | 8581 | 151 | 3461 | 7351 |
| 491 | 3271 | 8681 | 181 | 3631 | 7621 |
| 601 | 3571 | 3761 | 241 | 3701 | 7841 |
| 701 | 4091 | 8831 | 691 | 3851 | 7901 |
| 811 | 4801 | 8941 | 701 | 4051 | 8011 |
| 991 | 4871 | 8951 | 1021 | 4231 | 8111 |
| 1031 | 5081 | 9011 | 1031 | 4241 | 8161 |
| 1061 | 5231 | 9161 | 1051 | 4271 | 8311 |
| 1231 | 5521 | 9221 | 1151 | 4451 | 8431 |
| 1321 | 5581 | 9421 | 1181 | 4951 | 8521 |
| 1361 | 5641 | 9491 | 1291 | 5051 | 8741 |
| 1481 | 5741 | 9721 | 1531 | 5171 | 8761 |
| 1571 | 5981 | 9781 | 1811 | 5261 | 8821 |
| 1801 | 6131 | 9931 | 1901 | 5431 | 8851 |
| 1831 | 6361 |  | 2161 | 5521 | 9001 |
| 1861 | 6491 |  | 2251 | 5641 | 9161 |
| 2131 | 6761 |  | 2341 | 5741 | 9241 |
| 2221 | 7121 |  | 2531 | 5881 | 9281 |
| 2281 | 7211 |  | 2621 | 6011 | 9391 |
| 2351 | 7331 |  | 2731 | 6491 | 9491 |
| 2371 | 7481 |  | 2741 | 6551 | 9551 |
| 2381 | 7691 |  | 2791 | 6781 | 9501 |
| 2591 | 8161 |  | 3001 | 6841 | 9721 |
| 2571 | 8171 |  | 3181 | 6911 | 9851 |
| 2711 | 8311 |  | 3191 | 7211 |  |
|  |  |  |  |  |  |

values of $p$ are given in the accompanying tables. The lists of primes $p$ having 2 or 3 as a quintic residue of $p$ agree with those of Bickmore [1]. The corresponding densities are 0.1960..., 0.1862. . , 0.1895. . , 0.1797. . , 0.1830. . , 0.2124. . , 0.2189 . . , 0.2516 . ., which are in fair agreement with the asymptotic density $1 / 5$ $=0.2$ (see for example Elliott [4]).

The author would like to acknowledge his indebtedness to Messrs. Barry Lowe and Barry Savage for their help with the programming necessary for this paper.

Finally, we mention that the corresponding problem for eighth powers has been treated recently by von Lienen [11].

Department of Mathematics
Carleton University
Ottawa, Ontario, Canada

1. C. E. BICKMORE, "On the numerical factors of $a^{n}-1.11, "$ Messenger Math., v. 26, 1897, pp. 1-38.
2. A. J. C. CUNNINGHAM \& T. GOSSET, "4-tic and 3-tic residuacity tables," Messenger Math., v. 50, 1920, pp. 1-30.
3. L. E. DICKSON, "Cyclotomy, higher congruences, and Waring's problem," Amer. J. Math., v. 57, 1935, pp. 391-424.
4. P. D. T. A. ELLIOTT, "A problem of Erdös concerning power residue sums," Acta Arith., v. 13, 1967/68, pp. 131-149; Corrigendum, ibid., v. 14, 1967/68, p. 437. MR 36 \#3741; 37 \#4031.
5. K. G. J. JACOBI, "De residuis cubicis commentatio numerosa," J. Reine Angew. Math., v. 2, 1827, pp. 66-69.
6. E. E. KUMMER, "Über die Divisoren gewisser Formen der Zahlen, welche aus der Theorie der Kreistheilung enstehen,"J. Reine Angew. Math., v. 30, 1846, pp. 107-116.
7. EMMA LEHMER, "The quintic character of 2 and 3," Duke Math. J., v. 18, 1951, pp. 1118. MR 12, 677 .
8. EMMA LEHMER, "Criteria for cubic and quartic residuacity," Mathematika, v. 5, 1958, pp. 20-29. MR 20 \#1668.
9. EMMA LEHMER, "Artiads characterized," J. Math. Anal. Appl., v. 15, 1966, pp. $118-$ 131. MR 34 \#1261.
10. EMMA LEHMER, "On the divisors of the discriminant of the period equation," Amer. J. Math., v. 90, 1968, pp. 375-379. MR 37 \#2718.
11. H. von LIENEN, "Primzahlen als achte Potenzreste," J. Reine Angew. Math., v. 266, 1974, pp. 107-117. MR 49 \#4916.
12. G. B. MATHEWS, Theory of Numbers, 2nd ed., Chelsea, New York, 1961. MR 23 \#A3698.
13. J. B. MUSKAT, "Criteria for solvability of certain congruences," Canad. J. Math., v. 16, 1964, pp. 343-352. MR 29 \#1 170.
14. J. B. MUSKAT, 'On the solvability of $x^{e} \equiv e(\bmod p), "$ Pacific J. Math., v. 14, 1964, pp. 257-260. MR 28 \#2997.

[^0]:    Received March 27, 1975; revised October 16, 1975.
    AMS (MOS) subject classifications (1970). Primary 10A15; Secondary 12C20.
    Key words and phrases. Quintic residue, primitive root, $f$-nomial periods, period equation.
    ${ }^{*}$ Research supported under National Research Council of Canada Grant No. A-7233.

